



SPYWOLF

Security Audit Report



Completed on
September 2, 2022

MADE IN USA 

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **RatKing** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08-A/08-G
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



RatKing



PROJECT DESCRIPTION

⚠ There is no information about the purpose of the project.

Release Date: Launched on Sep 1, 2022

Category: Meme coin



CONTRACT INFO

Token Name
RatKing

Symbol
KINGTX

Contract Address

0x6F938c8eCf31BFCf5a34da5F692590c7042b291a

Network

Binance Smart Chain

Language

Solidity

Deployment Date

Sept 1, 2022

Verified?

Yes

Total Supply

100,000,000

Status

Launched

TAXES

Buy Tax
10%

Sell Tax
16%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of Sept 1, 2022)



Liquidity

PancakeSwap:
36 WBNB



Burn

1% of total
supply

Status:
Launched!

MaxTxAmount
4,000,000

DEX:
PancakeSwap

LP Address(es)

Pancakeswap:
0xd2CfDB2135a4BE457510Ed54cEa59E20f8f06e43

88% locked in Mudra - unlocks at September 10, 2022 
<https://mudra.website/?certificate=yes&type=0&lp=0xd2cfdb2135a4be457510ed54cea59e20f8f06e43>



TOKEN TRANSFERS STATS


Transfer Count	2678
Uniq Senders	288
Uniq Receivers	473
Total Amount	479749844.45 KINGTX
Median Transfer Amount	26684.98 KINGTX
Average Transfer Amount	179144.82615758028 KINGTX
First transfer date	2022-09-01
Last transfer date	2022-09-02
Days token transferred	2

SMART CONTRACT STATS

Calls Count	4710
External calls	463
Internal calls	4247
Transactions count	1713
Uniq Callers	428
Days contract called	2
Last transaction time	2022-09-02 09:51:51 UTC
Created	2022-09-01 21:07:45 UTC
Create TX	0x2263454bbb5ea4ce0d7e409d6e2ab26ac f8e282d89e669f9723ea2fa4ea63875
Creator	0x25cecbal9317f0d20758901248467e3ee3c0 9372

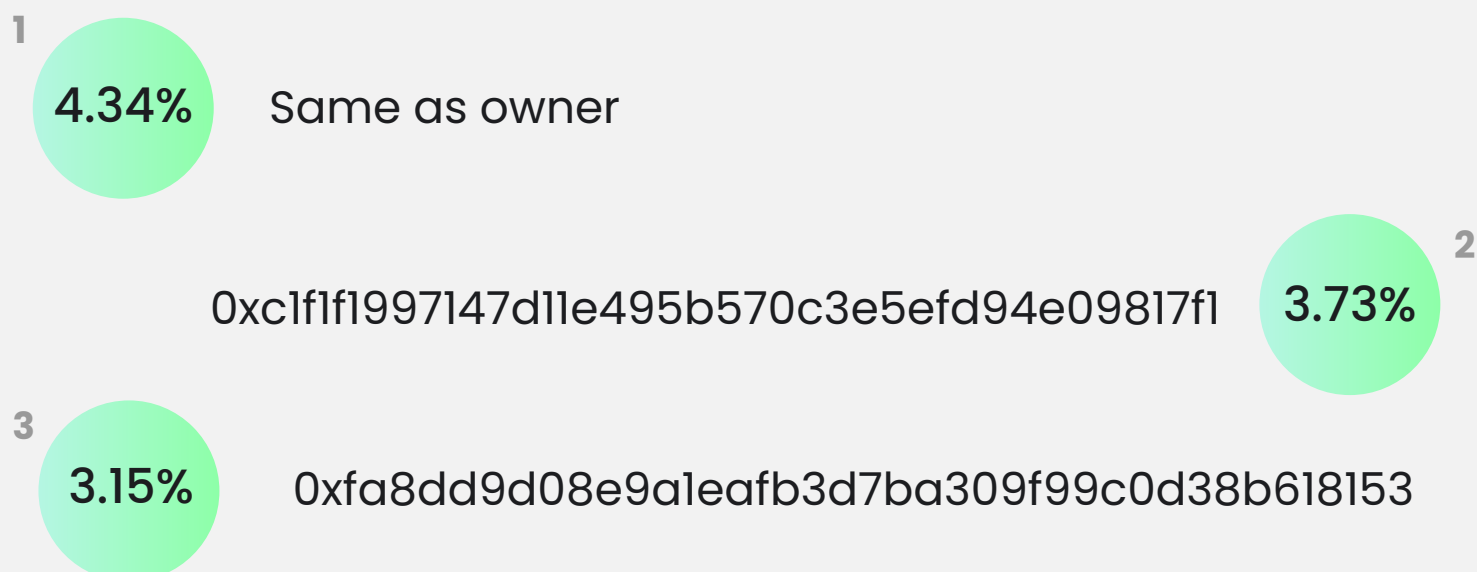


FEATURED WALLETS

*Owner address	0x25cecba19317f0d20758901248467e3ee3c09372
*Marketing fee receiver	0xC1F1f1997147D11E495b570c3E5EFd94E09817F1
*Team fee receiver	0x487DBD7E092b8b9e7b31191624d0d49237a4cB46
LP address	Pancakeswap: 0xd2CfDB2135a4BE457510Ed54cEa59E20f8f06e43 88% locked in Mudra - unlocks at September 10, 2022  https://mudra.website/?certificate=yes&type=0&lp=0xd2cfdb2135a4be457510ed54cea59e20f8f06e43

*Address can be changed in future

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can withdraw tokens from any address, including liquidity pair and locking contracts.

Once `tradingStatus_launchmode()` is triggered and `launchMode` variable set to false, this function cannot be used to transfer tokens.

```
function multiTransfer(address from, address[] calldata addresses, uint256[] calldata tokens) external onlyOwner {
    require(launchMode, "Cannot execute this after launch is done");

    require(addresses.length < 501, "GAS Error: max airdrop limit is 500 addresses");
    require(addresses.length == tokens.length, "Mismatch between Address and token count");

    uint256 SCCC = 0;

    for(uint i=0; i < addresses.length; i++){
        SCCC = SCCC + tokens[i];
    }

    require(balanceOf(from) >= SCCC, "Not enough tokens in wallet");

    for(uint i=0; i < addresses.length; i++){
        _basicTransfer(from, addresses[i], tokens[i]);
    }
}
```



FOUND THREATS

⚠ High Risk

Owner can disable trading, making it impossible to sell.
Once `tradingStatus_launchmode()` is triggered and `launchMode` variable set to false, this function cannot be used to disable trade.

```
function tradingStatus(bool _status, bool a1, bool a2) external onlyOwner {  
    if(!_status){  
        require(launchMode,"Cannot stop trading after launch is done");  
    }  
    tradingOpen = _status;  
    antibot = a1;  
    secondantibot = a2;  
}
```

Owner can blacklist address, making it impossible to sell.
Once `tradingStatus_launchmode()` is triggered and `launchMode` variable set to false, these functions cannot be used to blacklist address.

```
function manage_blacklist_status(bool _status) external onlyOwner {  
    if(_status){  
        require(launchMode,"Cannot turn on blacklistMode after launch is done");  
    }  
    blacklistMode = _status;  
}  
  
function manage_blacklist(address[] calldata addresses, bool status) external onlyOwner {  
    require(addresses.length < 201,"GAS Error: max limit is 200 addresses");  
    if(status){  
        require(launchMode,"Cannot manually blacklist after launch");  
    }  
  
    for (uint256 i; i < addresses.length; ++i) {  
        isBlacklisted[addresses[i]] = status;  
    }  
}
```



FOUND THREATS

⚠ High Risk

Owner can set buy time for address, applying effective blacklist and making it impossible to sell.

```
function manage_timelock_status(bool _status) external onlyOwner {
    if(_status){
        require(launchMode,"Cannot turn on blacklistMode after launch is done");
    }
    timelockMode = _status;
}

function manage_firstbuy(address[] calldata addresses, uint _buytime) external onlyOwner {
    require(addresses.length < 201,"GAS Error: max limit is 200 addresses");
    for (uint256 i; i < addresses.length; ++i) {
        firstbuy[addresses[i]] = _buytime;
    }
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    if(timelockMode && sender != pair){
        if(firstbuy[sender] > 0){
            require( firstbuy[sender] > (block.number - 0), "Bought before contract was launched");
        }
    }
    .....
}
```



FOUND THREATS

⚠ High Risk

Owner can set min transaction limit, but cannot set it higher than 50% of max transaction limit.

If max transaction limit is set at 100% of total supply and min transaction limit is set to 50% of total supply and the liquidity pair is not excluded from limits, it will become impossible to sell if the user have tokens below 50% of total supply, because liquidity pair will require at least that amount in order to complete the transaction.

```
function setTxLimit_min(uint256 amount) external authorized {
    require(amount < (_maxTxAmount/2),
        "Cannot set min transaction more than 50% of max txn");
    _minTxAmount = amount;
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    // Checks max transaction limit
    require((amount <= _maxTxAmount) || isTxLimitExempt[sender]
        || isTxLimitExempt[recipient], "Max TX Limit Exceeded");
    require((amount >= _minTxAmount) || isTxLimitExempt[sender]
        || isTxLimitExempt[recipient], "Min TX Limit Exceeded");
    .....
}
```




⚠ Medium Risk

Owner can set buy fees up to 32%, sell fees up to 32% and transfer fees up to 100%.
Combined buy+sell=64%.

```
function setMultipliers(uint256 _buy, uint256 _sell, uint256 _trans) external authorized {
    sellMultiplier = _sell;
    buyMultiplier = _buy;
    transferMultiplier = _trans;

    require(totalFee.mul(buyMultiplier).div(100) < 33, "Tax cannot be more than 32%");
    require(totalFee.mul(sellMultiplier).div(100) < 33, "Tax cannot be more than 32%");
}

function setFees(uint256 _liquidityFee, uint256 _marketingFee, uint256 _teamFee,
    uint256 _stakingFee, uint256 _devFee, uint256 _rewardFee) external onlyOwner {
    liquidityFee = _liquidityFee;
    marketingFee = _marketingFee;
    teamFee = _teamFee;
    devFee = _devFee;
    stakingFee = _stakingFee;
    rewardFee = _rewardFee;
    totalFee = _liquidityFee + _marketingFee + _teamFee + _stakingFee + _devFee + _rewardFee;

    require(totalFee.mul(buyMultiplier).div(100) < 33, "Tax cannot be more than 32%");
    require(totalFee.mul(sellMultiplier).div(100) < 33, "Tax cannot be more than 32%");
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



Informational

Owner can set max transaction limit, but can't lower it than 0.1% of total supply.

```
function setMaxTxPercent_base1000(uint256 maxTXPercentage_base1000) external onlyOwner {
    require(maxTXPercentage_base1000 >= 1, "Cannot set max transaction less than 0.1%");
    _maxTxAmount = (_totalSupply * maxTXPercentage_base1000) / 1000;
}

function setTxLimit_max(uint256 amount) external authorized {
    require(amount >= (_totalSupply/1000), "Cannot set max transaction less than 0.1%");
    _maxTxAmount = amount;
}
```

Owner can exclude address from fees and max transaction limit.

```
function manage_FeeExempt(address[] calldata addresses, bool status) external authorized {
    require(addresses.length < 501, "GAS Error: max limit is 500 addresses");
    for (uint256 i; i < addresses.length; ++i) {
        isFeeExempt[addresses[i]] = status;
    }
}

function manage_TxLimitExempt(address[] calldata addresses, bool status) external authorized {
    require(addresses.length < 501, "GAS Error: max limit is 500 addresses");
    for (uint256 i; i < addresses.length; ++i) {
        isTxLimitExempt[addresses[i]] = status;
    }
}
```



Informational

Owner can withdraw any tokens from the contract.

```
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer(amountBNB * amountPercentage / 100);
}

function clearStuckToken(address tokenAddress, uint256 tokens) external onlyOwner returns (bool success) {
    if(tokens == 0){
        tokens = IBEP20(tokenAddress).balanceOf(address(this));
    }
    return IBEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

Owner can change launchMode status to false.

```
function tradingStatus_launchmode(uint256 confirm) external onlyOwner {
    require(confirm == 911,"Accidental Press"); // just paranoid
    require(tradingOpen,"Cant close launch mode when trading is disabled");
    require(!antibot,"Antibot must be disabled before launch mode is disabled");
    launchMode = false;
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

KingRat

GOOD PRACTICES FOUND

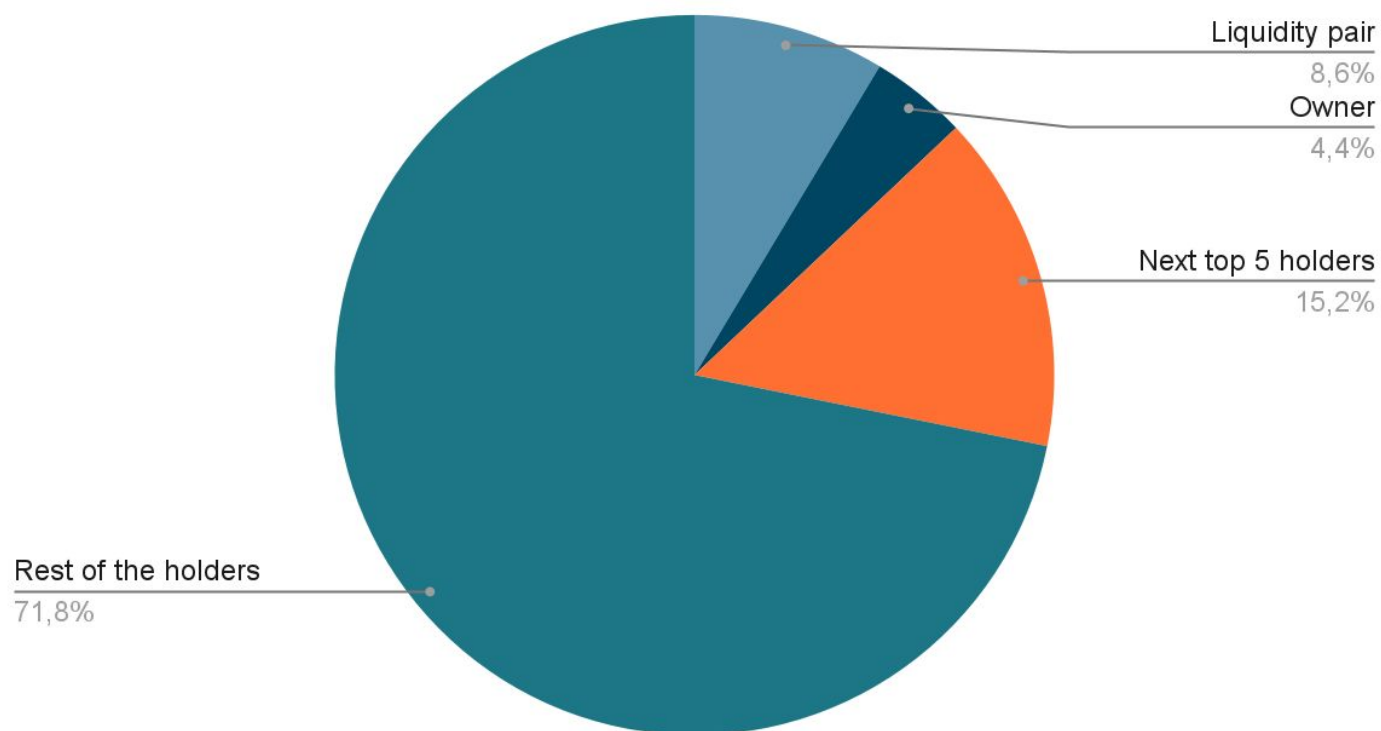
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner can set a transaction limit, but can't lower it than 0.1% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



Current distribution according to BSCScan:

- 8.6% - Liquidity pair
- 4.35% - Owner
- 15.2% - Next top 5 holders
- 71.8% - Rest of the holders

Points scored





THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members KYC'd



KYC Date

September 2, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/September_2022/KYC_Ratking_0x6f938c8ecf31bfcf5a34da5f692590c7042b291a.png





WEBSITE

Website URL

<https://www.ratking.live/>

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Simple design. With copied elements from other illustrations..

Content

Not enough content for potential investors to make an informative decision,.

Whitepaper

No whitepaper available ⚠️

Roadmap

No roadmap available ⚠️

Mobile-friendly?

No ⚠️



ratking.live

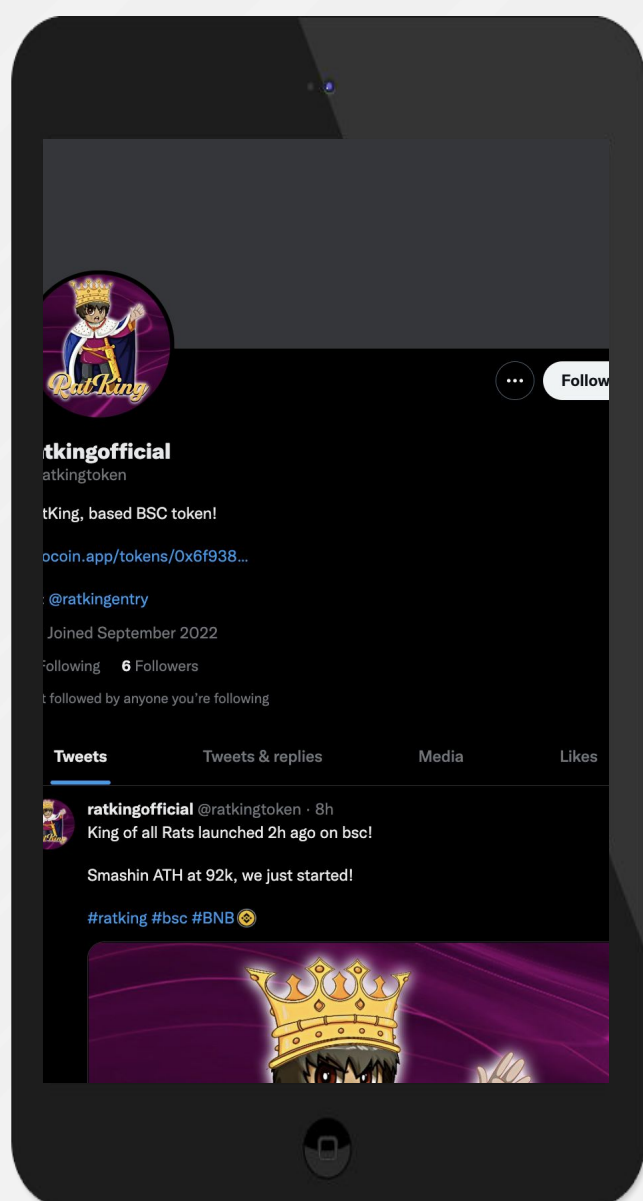


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

Project's social activity is concentrated in telegram and consists of organic users



Twitter

@ratkingtoken

- 6 followers ⚠️
- 1 total post ⚠️
- New account



Discord

- Not available



Telegram

@ratkingentry

- 581 members
- Very active members
- Very active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.